

FORM PTO-1390
(REV. 5-93)U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICEATTORNEY'S DOCKET NUMBER
2345/153**TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371**

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)

09/830784

INTERNATIONAL APPLICATION NO.
PCT/EP00/08263INTERNATIONAL FILING DATE
24 August 2000
(24.08.00)PRIORITY DATE CLAIMED:
1 September 1999
(01.09.99)TITLE OF INVENTION
METHOD FOR CLEARING CUSTOMER-SPECIFIC ENTITLEMENTS ON SECURITY MODULES IN CONDITIONAL
ACCESS SYSTEMS FOR PAY SERVICESAPPLICANT(S) FOR DO/EO/US
Rolf LAKOMY and Joerg SCHWENK

Applicant(s) herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) immediately rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
 - a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☒ has been transmitted by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
 - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ have been transmitted by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)) UNSIGNED.
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☒ A substitute specification and a marked up version of the substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: International Search Report and Form PCT/RO/101.

Express Mail No.:EL594612674US

U.S. APPLICATION NO. if known, see 37 C.F.R. 1.5

09/830784

INTERNATIONAL APPLICATION NO.
PCT/EP00/08263ATTORNEY'S DOCKET NUMBER
2345/15317. ☒ The following fees are submitted:**Basic National Fee (37 CFR 1.492(a)(1)-(5)):**

Search Report has been prepared by the EPO or JPO \$860.00

International preliminary examination fee paid to USPTO (37 CFR 1.482) \$690.00

No international preliminary examination fee paid to USPTO (37 CFR 1.482) but
international search fee paid to USPTO (37 CFR 1.445(a)(2)) \$710.00Neither international preliminary examination fee (37 CFR 1.482) nor international
search fee (37 CFR 1.445(a)(2)) paid to USPTO \$1,000.00International preliminary examination fee paid to USPTO (37 CFR 1.482) and all
claims satisfied provisions of PCT Article 33(2)-(4) \$100.00

CALCULATIONS | PTO USE ONLY

ENTER APPROPRIATE BASIC FEE AMOUNT =

\$ 860

Surcharge of \$130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months
from the earliest claimed priority date (37 CFR 1.492(e)).

\$

Claims	Number Filed	Number Extra	Rate	
Total Claims	10 - 20 =	0	X \$18.00	\$0
Independent Claims	2 - 3 =	0	X \$80.00	\$0
Multiple dependent claim(s) (if applicable)			+ \$270.00	\$

TOTAL OF ABOVE CALCULATIONS =

\$860

Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must
also be filed. (Note 37 CFR 1.9, 1.27, 1.28).

\$

SUBTOTAL =

\$860

Processing fee of \$130.00 for furnishing the English translation later the ☐ 20 ☐ 30
months from the earliest claimed priority date (37 CFR 1.492(f)).

\$

TOTAL NATIONAL FEE =

\$860

Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be
accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property

\$

TOTAL FEES ENCLOSED =

\$860

Amount to be
refunded

\$

charged

\$

- a. ☐ A check in the amount of \$ _____ to cover the above fees is enclosed.
- b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of \$860.00 to cover the above fees. A duplicate copy of this sheet is enclosed.
- c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:
Kenyon & Kenyon
One Broadway
New York, New York 10004
Telephone No. (212)425-7200
Facsimile No. (212)425-5288
CUSTOMER NO. 26646

SIGNATURE

Richard L. Mayer, Reg. No. 22,490
NAME

DATE

5/1/2001



26646

PATENT TRADEMARK OFFICE

09/830784

PTO/PCT Rec'd 01 MAY 2001

[2345/153]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s) : Rolf LAKOMY et al.
Serial No. : To Be Assigned
Filed : Herewith

For : METHOD FOR CLEARING CUSTOMER-SPECIFIC
ENTITLEMENTS ON SECURITY MODULES IN CONDITIONAL
ACCESS SYSTEMS FOR PAY SERVICES

Examiner : To Be Assigned
Art Unit : To Be Assigned

Assistant Commissioner
for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

SIR:

Please amend without prejudice the above-identified application before examination,
as follows.

IN THE TITLE:

Please replace the title with the following:

--METHOD FOR CLEARING CUSTOMER-SPECIFIC ENTITLEMENTS ON SECURITY
MODULES IN CONDITIONAL ACCESS SYSTEMS FOR PAY SERVICES--.

IN THE SPECIFICATION:

Please amend without prejudice the specification, including abstract, pursuant to the
attached substitute specification. Also attached is a marked up version of the substitute
specification, in which added text is shaded and in which deleted text is bracketed. No new matter
has been added.

EL594612674

IN THE CLAIMS:

Without prejudice, please cancel original claims 1 to 4, and please add new claims 5 to 14 as follows:

--5. (New) A method for clearing a customer-specific entitlement in a conditional access system to receive a chargeable service from a service provider by using a security module on which is stored at least one of a security algorithm and the customer-specific entitlement as at least one of a software program and data, the method comprising:

specifically assigning an EMM clearing signal to the security module to provide a specifically assigned EMM clearing signal; and

controlling a right-of-access by a customer through a service center, in response to a request from the service provider to the service center, using the specifically assigned EMM clearing signal by performing one of:

(i) an indirect clearing operation that includes the steps of:

(a) sending the specifically assigned EMM clearing signal from the service center to the service provider via at least one of a telephone system and a data communication system;

(b) feeding the specifically assigned EMM clearing signal for the chargeable service into a control unit of the service provider; and

(c) activating the security module via the control unit by using the specifically assigned EMM clearing signal; and

(ii) a direct clearing operation by sending the specifically assigned EMM clearing signal from the service center, with an assistance of a data transmission service in a digital broadcasting service, to the security module to clear the customer.

6. (New) The method of claim 5, wherein an electronically stored, service-specific credit balance is allocatable in monetary units to the security module.

7. (New) The method of claim 5, wherein in the indirect clearing operation of the security module of a querying customer, the data transmission service is provided by one of a fixed-line modem, a Global System for Mobile Communications (GSM) modem and a GSM-Service Management System (GSM-SMS) modem.

8. (New) The method of claim 5, wherein in the direct clearing operation of the security module of a querying customer:

an approximate location of the querying customer is found with the assistance of at least one of a digital cellular network and a mobile telephony network; and

the specifically assigned EMM clearing signal for clearing the querying customer is only routed into the digital broadcasting network in which the querying customer is situated at a time of a call and an ordering of the specifically assigned EMM clearing signal.

9. (New) The method of claim 5, wherein the chargeable service includes at least one of a pay TV service, a digital radio broadcasting service, a digital video broadcasting service, a service of a Society for Worldwide Interbank Financial Telecommunications and a video-on-demand service.

10. (New) An arrangement for clearing a customer-specific entitlement in a conditional access system to receive a chargeable service from a service provider by using a security module on which is stored at least one of a security algorithm and the customer-specific entitlement as at least one of a software program and data, the arrangement comprising:

an arrangement for specifically assigning an EMM clearing signal to the security module to provide a specifically assigned EMM clearing signal; and

an arrangement for controlling a right-of-access by a customer through a service center, in response to a request from the service provider to the service center, using the specifically assigned EMM clearing signal by performing one of:

(i) an indirect clearing operation that includes the steps of:

(a) sending the specifically assigned EMM clearing signal from the service center to the service provider via at least one of a telephone system and a data communication system;

(b) feeding the specifically assigned EMM clearing signal for the chargeable service into a control unit of the service provider; and

(c) activating the security module via the control unit by using the specifically assigned EMM clearing signal; and

(ii) a direct clearing operation by sending the specifically assigned EMM clearing signal from the service center, with an assistance of a data transmission service in a digital broadcasting service, to the security module to clear the customer.

11. (New) The arrangement of claim 10, wherein an electronically stored, service-specific credit balance is allocatable in monetary units to the security module.

12. (New) The arrangement of claim 10, wherein in the indirect clearing operation of the security module of a querying customer, the data transmission service is provided by one of a fixed-line modem, a Global System for Mobile Communications (GSM) modem and a GSM-Service Management System (GSM-SMS) modem.

13. (New) The arrangement of claim 10, wherein in the direct clearing operation of the security module of a querying customer:

an approximate location of the querying customer is found with the assistance of at least one of a digital cellular network and a mobile telephony network; and

the specifically assigned EMM clearing signal for clearing the querying customer is only routed into the digital broadcasting network in which the querying customer is situated at a time of a call and an ordering of the specifically assigned EMM clearing signal.

14. (New) The arrangement of claim 10, wherein the chargeable service includes at least one of a pay TV service, a digital radio broadcasting service, a digital video broadcasting service, a service of a Society for Worldwide Interbank Financial Telecommunications and a video-on-demand service.--.

REMARKS

This Preliminary Amendment cancels without prejudice original claims 1 to 4 in the underlying PCT Application No. PCT/EP00/08263, and adds without prejudice new claims 5 to 14. The new claims conform the claims to U.S. Patent and Trademark Office rules and does not add new matter to the application.

The amendments to the specification and abstract reflected in the substitute specification are to conform the specification and abstract to U.S. Patent and Trademark Office rules and to introduce changes made in the underlying PCT application, and do not introduce new matter into the application.

The underlying PCT Application No. PCT/EP00/08263 includes an International Search Report, issued December 22, 2000, a copy of which is included. The Search Report includes a list of documents that were considered by the Examiner in the underlying PCT application.

Applicants assert that the present invention is new, non-obvious, and useful. Prompt consideration and allowance of the claims are respectfully requested.

Respectfully Submitted,
KENYON & KENYON

Dated: 5/1/2001

By: 

Richard L. Mayer
(Reg. No. 22,490)

One Broadway
New York, NY 10004
(212) 425-7200
(212) 425-5288

CUSTOMER NO. 26646

*By AD
Reg. No.
33,805
Javan
P(EO) (ET)*

370564v2

METHOD FOR CLEARING CUSTOMER-SPECIFIC ENTITLEMENTS ON SECURITY
MODULES IN CONDITIONAL ACCESS SYSTEMS FOR PAY SERVICES

Field Of The Invention

The present invention is directed to a method for clearing customer-specific entitlements or rights of access in conditional access systems, to receive chargeable services, such as pay TV, digital broadcasting data services in the Digital Audio Broadcasting (DAB), Digital Video Broadcasting (DVB), Society for Worldwide Interbank Financial Telecommunications (SWIFT), video-on-demand, as well as any other digital services broadcast via radio broadcasting systems, with the use of security modules, such as smart cards, on which security algorithms and/or customer-specific entitlements are stored in the form of software programs and data.

Background Information

Security modules in the form of smart cards are already in use today in various sectors where people, or machines, need to be granted authorized or conditional access, e.g., conditional access (CA systems), to data, programs, or to other machines, when stipulated conditions or entitlements are satisfied, e.g., pay TV. Other areas of application for smart cards may include electronic payment arrangements, GSM telephony (global system for mobile telecommunications, European digital cellular standard), or digital broadcasting data services in the DAB, DVB, SWIFT, and also, in the future, video-on-demand.

In modern conditional access systems, access is controlled almost exclusively through the use of smart cards that utilize chip card technology. These smart cards may contain stored security algorithms and customer-specific entitlements to receive fee-based data services. In conditional access systems, content providers may encounter the problem of

8LS94612674

wanting to reach more than one customer, but not all of them. Only authorized customers should be able to receive a service. These are customers who meet stipulated conditions by purchasing entitlements, for example by paying a monthly
5 subscriber fee. Radio broadcast systems are used to transmit entitlements of this kind. Therefore, it is believed that there is a need to control access to certain information which is disseminated over broadcasting systems, but that, in principle, can be received by everyone.

10 Conditional access systems, such as pay TV, protect such information from unauthorized access by scrambling, i.e., encrypting the program contents, by storing authorization to receive in the terminal's security module, and by adding
15 receive conditions to the program. The terminals used to receive a pay TV program may include the so-called set-top boxes or decoders. Other types of terminals may include mobile receivers, PC cards, or PCMCIA (Personal Computer Memory Card International Association) modules. The terminal can also be
20 integrated in the television set. In various cases, however, the lack of a way to guarantee receipt may make problematic the clearing of smart cards in broadcast systems, particularly when they are used in mobile devices for receiving services that do not feature point-to-point connections, as telephones
25 do.

A customer cannot utilize a desired service until the card is cleared, immediately following acquisition of the card. However, the sender of a clearing or signal may not have any
30 information on whether his clearing was actually received by the customer. A clearing is not effected when the unit being used is not able to receive a broadcast. This is the case, for example, in underground garages shielded by buildings, or when a radio communications network needed for sending out
35 entitlements is not yet completely built up. In these cases, entitlements, constituted as so-called Entitlement Management Messages (EMM messages), cannot be received on an area-wide

basis. In contrast, a controlled first clearing, including acknowledgment message, can be very reliable and also renders possible an instantaneous collection of charges for the cleared service at the instant of its acquisition.

5

Program contents are scrambled, in that the data are encoded by an encryption algorithm, with the control of a so-called control word CW. The algorithm mainly used in Europe for digital television based on the MPEG-2 standard (digital code standard of the Moving Picture Expert Group) is the DVB common scrambling algorithm. Other algorithms, however, such as Data Encryption Standard (DES) or triple DES, inter alia, (see Bruce Schneier, Angewandte Kryptographie, [Applied Cryptography], Wiley, 1996) may also be used.

15

In "Entitlement Control Messages" (ECM), a decoder or other receiver module is not only informed of new control words (CW), but also of the conditions under which a program may be received. Since both the CW, as well as the receive conditions, depend on the particular service, ECMs are allocated to each service. Once an ECM is received, it is directly routed to the security module. The control word CW must be transmitted confidentially. To protect the ECM, cryptographic methods are employed. Since the ECMs are sent to all customers, all authorized customers must possess the same key in order to decode the control word cryptogram. This is referred to as service key SK. The control word CW should be changed at relatively brief intervals, to make it impossible to recognize scrambling patterns.

30

Entitlement Management Messages (EMM) are used to set and to change receive entitlements stored in the decoder or in the security module. EMM messages must be sent to the individual address of the customer (respectively, of the decoder or of the security module). The customer's address and EMM messages must be protected from change; it must be ensured that only the program provider is able to generate EMM messages.

35

Individual addresses always appear in the EMM messages as unencrypted messages; piracy protection can only be achieved by using supplementary information that is stored so as to be unreadable for the customer. This is the personal key (PK), which is linked to the customer address. The EMM messages are sent via the same broadcast system as the payload data. The EMM messages are not permanently linked to the program content, but rather to the logical address of the customer's terminal, respectively to that of the security module, so that EMM can be addressed to individual customers or to groups of customers. Moreover, for the use of specific services, such as mobile received services or pay-per-view, a backward channel can be available, which is either implemented manually (call at a service center) or automatically, e.g., connection from the decoder to the transmission center via TCP/IP (Transmission Control Protocol/Internet Protocol).

Entitlements can change when, for example, customers' chargeable accounts are not settled. The consequence of this can be the blocking of a receive authorization, for example. EMMs can also be used, however, for activating or reactivating services on smart cards. In these cases, the entitlements must be reset in the security module, such as the smart card. Today, as security modules, chip cards are mostly used which are not permanently connected to the terminal, but rather which can be removed from the terminal and replaced. (See, e.g., Bernd Seiler, Taschenbuch der Telekom Praxis, 1996, Schiele & Schön Berlin 1996; Jörg Schwenk, "Conditional Access" or "Wie kann man den Zugriff auf Rundfunksendungen kontrollieren?").

Moreover, with the introduction of new transmission media, such as DAB and DVB-T, pay services are gaining in importance for mobile customers, as well. These are customers, who, for example, carry a terminal along with them in their automobile. Here, however, the following problems may arise:

- the data capacity of the services is limited (e.g., DAB, Swift, among other things);
- the receive situation is difficult (e.g., not yet fully developed broadcasting networks or automobiles located in underground garages); or
- a backward channel is normally not available.

Summary Of The Invention

An exemplary method and/or exemplary arrangement of the present invention is directed to providing a method for an authorized customer's chip card to be made individually addressable to facilitate any change in pay services, and/or to further providing that the pay services are serviceable for mobile customers as well.

Detailed Description

An exemplary method and/or exemplary arrangement of the present invention provides that, in response to a request from a service provider, i.e., an institution, such as a T-Point, authorized to issue or sell security modules, to a service center responsible for controlling rights-of-access, e.g., a data service center in the DAB, in the case of indirect clearing, the service center sends an EMM clearing signal, specifically allocated to this security module, either via the telephone or a data communications system, to the service provider, and, there, feeds this EMM clearing signal for the service in question into a control unit of the service provider, and the security module is activated via the control unit by this EMM clearing signal assigned to it, or, in the case of direct clearing, the service center, with the aid of a data transmission service in a digital broadcasting service, such as the DAB single-frequency network, transmits the specifically assigned EMM clearing signal to the security module of the customer making the request and clears this customer.

In the case of a direct clearing, a service on a security

module, such as a smart card, can be cleared by the particular transmission system, such as by using commercial DAB or DVB receivers themselves, or, in the case of an indirect clearing, with the aid of another service, besides the transmitting service. Following payment of the relevant data service fee, the service center assigns the entitlement by implementing a direct or indirect clearing, as mentioned above, via the smart-card specific EMM. A control unit set up at the service provider confirms activation of the security module, for instance of a smart card, for the service in question.

In another exemplary embodiment and/or exemplary method of the present invention, in the case of direct and indirect clearing, an electronically stored, service-specific credit balance (tokens) are allocated in monetary units to the security module.

In another exemplary embodiment and/or exemplary method of the present invention, in the case of indirect clearing of the security module of the querying customer, the data transmission service is believed to be advantageously carried out, e.g., via a fixed-line modem, via a GSM (Global System for Mobile Communications) modem or via GSM-SMS services (where SMS is an acronym for "Service Management System").

In the case of direct clearing of the querying customer's security module, the approximate location of the customer can be found with the assistance of the cellular network, for example, the GSM network, the customer is using. The specific EMM clearing signal for clearing the customer can be routed just within the DAM single-frequency network, where the customer is located at the time of the call and of the ordering of the EMM clearing signal.

An exemplary embodiment and/or exemplary method of the present invention may implement a backward channel using GSM. In this regard, the sequence is described based on the DAB example:

(i) From his or her automobile, via GSM, for example, the customer signals the data service center in the DAB requesting a clearing, for example, for a single data service or for a subscription, or in the case of non-receipt, a clearing, or an allocation of electronic, service-specific credit (tokens) on the smart card.

(ii) In the data service center in the DAB, in collaboration, for example, with a GSM carrier, e.g., T-Mobil, the GSM cell, respectively, in this manner, the DAB single-frequency network that covers a wider area, is determined in which the caller is located at the very moment.

(iii) The relevant EMM is routed, with the clearing, to the DAB single-frequency network where the subscriber is located.

An exemplary embodiment and/or method of the present invention may further provide that there is no need to broadcast EMMs on a country-wide basis, but still only locally in the DAB service areas where the subscriber is also located. It is believed that this makes the data rate required for the EMMs substantially lower. In the case of a call, it is ensured that the caller can also receive the EMM, since, from an established GSM connection, one can infer the possibility of DAB reception. Further, according to an exemplary embodiment and/or exemplary method of the present invention, a backward channel can be provided for new services.

In this context, the EMMs are not sent, for example, over a GSM channel, since this would presuppose a data connection between the mobile telephone and the DAB receiver, which is, however, theoretically conceivable.

The exemplary embodiment and/or exemplary method in accordance with the present invention is believed to have industrial applicability, in particular for clearing customer-specific access entitlements in Conditional Access Systems to enable chargeable media services to be received.

Abstract Of The Disclosure

A method for clearing customer-specific entitlements in conditional access systems, to receive chargeable media services, with the use of security modules, such as smart cards, on which security algorithms and/or customer-specific entitlements are stored in the form of software programs. In response to a request from a service provider, such as a T-Point or other institution authorized to sell security modules, in an indirect clearing, the service center responsible for controlling entitlements sends an EMM clearing signal, specifically allocated to this security module, either via the telephone or a data communications system, to the service provider, where this EMM clearing signal for the media service in question is fed into a control unit of the service provider, and the security module is activated via the control unit by this EMM clearing signal assigned to it. In a direct clearing, the service center, with the assistance of a further data transmission service in a digital broadcasting service, such as the DAB single-frequency network, transmits the specifically assigned EMM clearing signal to the security module of the customer making the request and clears this customer.

METHOD FOR CLEARING CUSTOMER-SPECIFIC ENTITLEMENTS ON SECURITY
MODULES IN CONDITIONAL ACCESS SYSTEMS FOR PAY SERVICES

Field [o]Of [t]The Invention

[

]The present invention is directed to a method for clearing
customer-specific entitlements []or rights of access in
conditional access systems, to receive chargeable[] services,
such as pay TV, digital broadcasting data services in the
[DAB, DVB, Swift]Digital Audio Broadcasting (DAB), Digital
Video Broadcasting (DVB), Society for Worldwide Interbank
Financial Telecommunications (SWIFT), video-on-demand, as well
as any other digital services broadcast via radio broadcasting
systems, with the use of security modules, such as smart
cards, on which security algorithms and/or customer-specific
entitlements are stored in the form of software programs and
data[, according to the definition of the species in Claim 1].

Background Information[

1

Security modules in the form of smart cards are already in use
today in [many]various sectors where people, or machines[as
well], need to be granted authorized or conditional access[
[]e.g., conditional access (CA systems)[], to data,
programs, or to other machines, when stipulated conditions or
entitlements are satisfied[(],e.g., pay TV[])]. Other[
typical] areas of application for smart cards may include
electronic payment arrangements, GSM telephony (global system
for mobile telecommunications, European digital cellular
standard), or digital broadcasting data services in the DAB,
DVB, [Swift]SWIFT, and also, in the future, video-on-demand.

In modern conditional access systems, access is controlled
almost exclusively through the use of smart cards that utilize

EL594612674

MARKED UP VERSION OF THE SUBSTITUTE SPECIFICATION

chip card technology. These smart cards may contain stored security algorithms and customer-specific entitlements to receive fee-based[] data services. In conditional access systems, content providers may encounter the problem of[
5 certainly] wanting to reach more than one customer, but not all of them. Only authorized customers should be able to receive a service. These are customers who meet stipulated conditions by purchasing entitlements, for example by paying a monthly subscriber fee. Radio broadcast systems are used to
10 transmit entitlements of this kind. Therefore, it is believed that there is a need to control access to certain information which is disseminated over broadcasting systems, but that, in principle, can be received by everyone.

Conditional access systems, such as pay TV, protect such information from unauthorized access by scrambling, i.e., encrypting the program contents, by storing authorization to receive[entitlement] in the terminal's security module, and by adding receive conditions to the program. The terminals [usually]used to receive a pay TV program [are]may include the so-called set-top boxes or decoders. Other types of terminals [are also possible, such as]may include mobile receivers, PC cards, or PCMCIA[] (Personal Computer Memory Card International Association) modules. The terminal can also
25 be integrated in the television set. In [many]various cases, however, the lack of a way to guarantee receipt [makes]may make problematic the clearing of smart cards[problematic] in broadcast systems, particularly when they are used in mobile devices for receiving services that do not feature
30 point-to-point connections, as telephones do.[]

A customer cannot utilize a desired service until the card is cleared, immediately following acquisition of the card. However, the sender of a clearing or signal [usually does]may
35 not have any information on whether his clearing[]was actually received by the customer. A clearing is not effected

when the unit being used is not able to receive a broadcast. This is the case, for example, in underground garages shielded by buildings, or when a radio communications network needed for sending out entitlements is not yet completely built up.

5 In these cases, entitlements, constituted as so-called [EMM messages (Entitlement Management Messages (EMM messages), cannot be received on an area-wide basis. In contrast, a controlled first clearing, including acknowledgment message, [is] can be very reliable and also renders possible an
10 instantaneous collection of charges for the cleared service at the instant of its acquisition.

5
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995
1000
1005
1010
1015
1020
1025
1030
1035
1040
1045
1050
1055
1060
1065
1070
1075
1080
1085
1090
1095
1100
1105
1110
1115
1120
1125
1130
1135
1140
1145
1150
1155
1160
1165
1170
1175
1180
1185
1190
1195
1200
1205
1210
1215
1220
1225
1230
1235
1240
1245
1250
1255
1260
1265
1270
1275
1280
1285
1290
1295
1300
1305
1310
1315
1320
1325
1330
1335
1340
1345
1350
1355
1360
1365
1370
1375
1380
1385
1390
1395
1400
1405
1410
1415
1420
1425
1430
1435
1440
1445
1450
1455
1460
1465
1470
1475
1480
1485
1490
1495
1500
1505
1510
1515
1520
1525
1530
1535
1540
1545
1550
1555
1560
1565
1570
1575
1580
1585
1590
1595
1600
1605
1610
1615
1620
1625
1630
1635
1640
1645
1650
1655
1660
1665
1670
1675
1680
1685
1690
1695
1700
1705
1710
1715
1720
1725
1730
1735
1740
1745
1750
1755
1760
1765
1770
1775
1780
1785
1790
1795
1800
1805
1810
1815
1820
1825
1830
1835
1840
1845
1850
1855
1860
1865
1870
1875
1880
1885
1890
1895
1900
1905
1910
1915
1920
1925
1930
1935
1940
1945
1950
1955
1960
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
2020
2025
2030
2035
2040
2045
2050
2055
2060
2065
2070
2075
2080
2085
2090
2095
2100
2105
2110
2115
2120
2125
2130
2135
2140
2145
2150
2155
2160
2165
2170
2175
2180
2185
2190
2195
2200
2205
2210
2215
2220
2225
2230
2235
2240
2245
2250
2255
2260
2265
2270
2275
2280
2285
2290
2295
2300
2305
2310
2315
2320
2325
2330
2335
2340
2345
2350
2355
2360
2365
2370
2375
2380
2385
2390
2395
2400
2405
2410
2415
2420
2425
2430
2435
2440
2445
2450
2455
2460
2465
2470
2475
2480
2485
2490
2495
2500
2505
2510
2515
2520
2525
2530
2535
2540
2545
2550
2555
2560
2565
2570
2575
2580
2585
2590
2595
2600
2605
2610
2615
2620
2625
2630
2635
2640
2645
2650
2655
2660
2665
2670
2675
2680
2685
2690
2695
2700
2705
2710
2715
2720
2725
2730
2735
2740
2745
2750
2755
2760
2765
2770
2775
2780
2785
2790
2795
2800
2805
2810
2815
2820
2825
2830
2835
2840
2845
2850
2855
2860
2865
2870
2875
2880
2885
2890
2895
2900
2905
2910
2915
2920
2925
2930
2935
2940
2945
2950
2955
2960
2965
2970
2975
2980
2985
2990
2995
3000
3005
3010
3015
3020
3025
3030
3035
3040
3045
3050
3055
3060
3065
3070
3075
3080
3085
3090
3095
3100
3105
3110
3115
3120
3125
3130
3135
3140
3145
3150
3155
3160
3165
3170
3175
3180
3185
3190
3195
3200
3205
3210
3215
3220
3225
3230
3235
3240
3245
3250
3255
3260
3265
3270
3275
3280
3285
3290
3295
3300
3305
3310
3315
3320
3325
3330
3335
3340
3345
3350
3355
3360
3365
3370
3375
3380
3385
3390
3395
3400
3405
3410
3415
3420
3425
3430
3435
3440
3445
3450
3455
3460
3465
3470
3475
3480
3485
3490
3495
3500
3505
3510
3515
3520
3525
3530
3535
3540
3545
3550
3555
3560
3565
3570
3575
3580
3585
3590
3595
3600
3605
3610
3615
3620
3625
3630
3635
3640
3645
3650
3655
3660
3665
3670
3675
3680
3685
3690
3695
3700
3705
3710
3715
3720
3725
3730
3735
3740
3745
3750
3755
3760
3765
3770
3775
3780
3785
3790
3795
3800
3805
3810
3815
3820
3825
3830
3835
3840
3845
3850
3855
3860
3865
3870
3875
3880
3885
3890
3895
3900
3905
3910
3915
3920
3925
3930
3935
3940
3945
3950
3955
3960
3965
3970
3975
3980
3985
3990
3995
4000
4005
4010
4015
4020
4025
4030
4035
4040
4045
4050
4055
4060
4065
4070
4075
4080
4085
4090
4095
4100
4105
4110
4115
4120
4125
4130
4135
4140
4145
4150
4155
4160
4165
4170
4175
4180
4185
4190
4195
4200
4205
4210
4215
4220
4225
4230
4235
4240
4245
4250
4255
4260
4265
4270
4275
4280
4285
4290
4295
4300
4305
4310
4315
4320
4325
4330
4335
4340
4345
4350
4355
4360
4365
4370
4375
4380
4385
4390
4395
4400
4405
4410
4415
4420
4425
4430
4435
4440
4445
4450
4455
4460
4465
4470
4475
4480
4485
4490
4495
4500
4505
4510
4515
4520
4525
4530
4535
4540
4545
4550
4555
4560
4565
4570
4575
4580
4585
4590
4595
4600
4605
4610
4615
4620
4625
4630
4635
4640
4645
4650
4655
4660
4665
4670
4675
4680
4685
4690
4695
4700
4705
4710
4715
4720
4725
4730
4735
4740
4745
4750
4755
4760
4765
4770
4775
4780
4785
4790
4795
4800
4805
4810
4815
4820
4825
4830
4835
4840
4845
4850
4855
4860
4865
4870
4875
4880
4885
4890
4895
4900
4905
4910
4915
4920
4925
4930
4935
4940
4945
4950
4955
4960
4965
4970
4975
4980
4985
4990
4995
5000
5005
5010
5015
5020
5025
5030
5035
5040
5045
5050
5055
5060
5065
5070
5075
5080
5085
5090
5095
5100
5105
5110
5115
5120
5125
5130
5135
5140
5145
5150
5155
5160
5165
5170
5175
5180
5185
5190
5195
5200
5205
5210
5215
5220
5225
5230
5235
5240
5245
5250
5255
5260
5265
5270
5275
5280
5285
5290
5295
5300
5305
5310
5315
5320
5325
5330
5335
5340
5345
5350
5355
5360
5365
5370
5375
5380
5385
5390
5395
5400
5405
5410
5415
5420
5425
5430
5435
5440
5445
5450
5455
5460
5465
5470
5475
5480
5485
5490
5495
5500
5505
5510
5515
5520
5525
5530
5535
5540
5545
5550
5555
5560
5565
5570
5575
5580
5585
5590
5595
5600
5605
5610
5615
5620
5625
5630
5635
5640
5645
5650
5655
5660
5665
5670
5675
5680
5685
5690
5695
5700
5705
5710
5715
5720
5725
5730
5735
5740
5745
5750
5755
5760
5765
5770
5775
5780
5785
5790
5795
5800
5805
5810
5815
5820
5825
5830
5835
5840
5845
5850
5855
5860
5865
5870
5875
5880
5885
5890
5895
5900
5905
5910
5915
5920
5925
5930
5935
5940
5945
5950
5955
5960
5965
5970
5975
5980
5985
5990
5995
6000
6005
6010
6015
6020
6025
6030
6035
6040
6045
6050
6055
6060
6065
6070
6075
6080
6085
6090
6095
6100
6105
6110
6115
6120
6125
6130
6135
6140
6145
6150
6155
6160
6165
6170
6175
6180
6185
6190
6195
6200
6205
6210
6215
6220
6225
6230
6235
6240
6245
6250
6255
6260
6265
6270
6275
6280
6285
6290
6295
6300
6305
6310
6315
6320
6325
6330
6335
6340
6345
6350
6355
6360
6365
6370
6375
6380
6385
6390
6395
6400
6405
6410
6415
6420
6425
6430
6435
6440
6445
6450
6455
6460
6465
6470
6475
6480
6485
6490
6495
6500
6505
6510
6515
6520
6525
6530
6535
6540
6545
6550
6555
6560
6565
6570
6575
6580
6585
6590
6595
6600
6605
6610
6615
6620
6625
6630
6635
6640
6645
6650
6655
6660
6665
6670
6675
6680
6685
6690
6695
6700
6705
6710
6715
6720
6725
6730
6735
6740
6745
6750
6755
6760
6765
6770
6775
6780
6785
6790
6795
6800
6805
6810
6815
6820
6825
6830
6835
6840
6845
6850
6855
6860
6865
6870
6875
6880
6885
6890
6895
6900
6905
6910
6915
6920
6925
6930
6935
6940
6945
6950
6955
6960
6965
6970
6975
6980
6985
6990
6995
7000
7005
7010
7015
7020
7025
7030
7035
7040
7045
7050
7055
7060
7065
7070
7075
7080
7085
7090
7095
7100
7105
7110
7115
7120
7125
7130
7135
7140
7145
7150
7155
7160
7165
7170
7175
7180
7185
7190
7195
7200
7205
7210
7215
7220
7225
7230
7235
7240
7245
7250
7255
7260
7265
7270
7275
7280
7285
7290
7295
7300
7305
7310
7315
7320
7325
7330
7335
7340
7345
7350
7355
7360
7365
7370
7375
7380
7385
7390
7395
7400
7405
7410
7415
7420
7425
7430
7435
7440
7445
7450
7455
7460
7465
7470
7475
7480
7485
7490
7495
7500
7505
7510
7515
7520
7525
7530
7535
7540
7545
7550
7555
7560
7565
7570
7575
7580
7585
7590
7595
7600
7605
7610
7615
7620
7625
7630
7635
7640
7645
7650
7655
7660
7665
7670
7675
7680
7685
7690
7695
7700
7705
7710
7715
7720
7725
7730
7735
7740
7745
7750
7755
7760
7765
7770
7775
7780
7785
7790
7795
7800
7805
7810
7815
7820
7825
7830
7835
7840
7845
7850
7855
7860
7865
7870
7875
7880
7885
7890
7895
7900
7905
7910
7915
7920
7925
7930
7935
7940
7945
7950
7955
7960
7965
7970
7975
7980
7985
7990
7995
8000
8005
8010
8015
8020
8025
8030
8035
8040
8045
8050
8055
8060
8065
8070
8075
8080
8085
8090
8095
8100
8105
8110
8115
8120
8125
8130
8135
8140
8145
8150
8155
8160
8165
8170
8175
8180
8185
8190
8195
8200
8205
8210
8215
8220
8225
8230
8235
8240
8245
8250
8255
8260
8265
8270
8275
8280
8285
8290
8295
8300
8305
8310
8315
8320
8325
8330
8335
8340
8345
8350
8355
8360
8365
8370
8375
8380
8385
8390
8395
8400
8405
8410
8415
8420
8425
8430
8435
8440
8445
8450
8455
8460
8465
8470
8475
8480
8485
8490
8495
8500
8505
8510
8515
8520
8525
8530
8535
8540
8545
8550
8555
8560
8565
8570
8575
8580
8585
8590
8595
8600
8605
8610
8615
8620
8625
8630
8635
8640
8645
8650
8655
8660
8665
8670
8675
8680
8685
8690
8695
8700
8705
8710
8715
8720
8725
8730
8735
8740
8745
8750
8755
8760
8765
8770
8775
8780
8785
8790
8795
8800
8805
8810
8815
8820
8825
8830
8835
8840
8845
8850
8855
8860
8865
8870
8875
8880
8885
8890
8895
8900
8905
8910
8915
8920
8925
8930
8935
8940
8945
8950
8955
8960
8965
8970
8975
8980
8985
8990
8995
9000
9005
9010
9015
9020
9025
9030
9035
9040
9045
9050
9055
9060
9065
9070
9075
9080
9085
9090
9095
9100
9105
9110
9115
9120
9125
9130
9135
9140
9145
9150
9155
9160
9165
9170
9175
9180
9185
9190
9195
9200
9205
9210
9215
9220
9225
9230
9235
9240
9245
9250
9255
9260
9265
9270
9275
9280
9285
9290
9295
9300
9305
9310
9315
9320
9325
9330
9335
9340
9345
9350
9355
9360
9365
9370
9375
9380
9385
9390
9395
9400
9405
9410
9415
9420
9425
9430
9435
9440
9445
9450
9455
9460
9465
9470
9475
9480
9485
9490
9495
9500
9505
9510
9515
9520
9525
9530
9535
9540
9545
9550
9555
9560
9565
9570
9575
9580
9585
9590
9595
9600
9605
9610
9615
9620
9625
9630
9635
9640
9645
9650
9655
9660
9665
9670
9675
9680
9685
9690
9695
9700
9705
9710
9715
9720
9725
9730
9735
9740
9745
9750
9755
9760
9765
9770
9775
9780
9785
9790
9795
9800
9805
9810
9815
9820
9825
9830
9835
9840
9845
9850
9855
9860
9865
9870
9875
9880
9885
9890
9895
9900
9905
9910
9915
9920
9925
9930
9935
9940
9945
9950
9955
9960
9965
9970
9975
9980
9985
9990
9995
10000
10005
10010
10015
10020
10025
10030
10035
10040
10045
10050
10055
10060
10065
10070
10075
10080
10085
10090
10095
10100
10105
10110
10115
10120
10125
10130
10135
10140
10145
10150
10155
10160
10165
10170
10175
10180
10185
10190
10195
10200
10205
10210
10215
10220
10225
10230
10235
10240
10245
10250
10255
10260
10265
10270
10275
102

to recognize scrambling patterns.

Entitlement Management Messages (EMM) are used to set and to change receive entitlements stored in the decoder or in the security module. EMM messages must be sent to the individual address of the customer (respectively, of the decoder or of the security module). The customer's address and EMM messages must be protected from change; it must be ensured that only the program provider is able to generate EMM messages.

Individual addresses always appear in the EMM messages as unencrypted messages; piracy protection can only be achieved by using supplementary information that is stored so as to be unreadable for the customer. This is the personal key (PK), which is linked to the customer address. The EMM messages are sent via the same broadcast system as the payload data. The EMM messages are not permanently linked to the program content, but rather to the logical address of the customer's terminal, respectively to that of the security module, so that EMM can be addressed to individual customers or to groups of customers. Moreover, for the use of specific services, such as mobile received services or pay-per-view, a backward channel can be available, which is either implemented manually (call at a service center) or automatically (e.g., connection from the decoder to the transmission center via TCP/IP (Transmission Control Protocol/Internet Protocol)).

Entitlements can change when, for example, customers' chargeable accounts are not settled. The consequence of this can be the blocking of a receive authorization, for example. EMMs can also be used, however, for activating or reactivating services on smart cards. In these cases, the entitlements must be reset in the security module, such as the smart card. Today, as security modules, chip cards are mostly used which are not permanently connected to the terminal, but rather which can be removed from the terminal and replaced.

Reference is made to the related art publication in Bernd Seiler (publisher): taschenbuch der telekom praxis,] (See, e.g., Bernd Seiler, Taschenbuch der Telekom Praxis, 1996, Schiele & Schön Berlin 1996[,], Jörg Schwenk[:], "Conditional Access" or "Wie kann man den Zugriff auf Rundfunksendungen kontrollieren?"[]).

Moreover, with the introduction of new transmission media, such as DAB and DVB-T, pay services are gaining in importance for mobile customers, as well. These are customers, who, for example, carry a terminal along with them in their automobile. Here, however, the following problems may arise:

- the data capacity of the services is limited (e.g., DAB, Swift, [inter alia]among other things);
- the receive situation is difficult (e.g., not yet fully developed broadcasting networks or automobiles located in underground garages); or
- a backward channel is normally not available.

[Technical Objective

]Summary Of The [object]Invention

An exemplary method and/or exemplary arrangement of the present invention is[, therefore,] directed to [provide]providing a method[which will make it possible] for an authorized customer's chip card to be made individually addressable to facilitate any change in pay services, [the intention also being]and/or to further providing t[o make]hat the pay services are serviceable for mobile customers as well.

[Summary of the Invention

The object is achieved in]Detailed Description

An exemplary method and/or exemplary arrangement of the present invention provides that, in response to a request from

a service provider, i.e., an institution, such as a T-Point, authorized to issue or sell security modules, to a service center responsible for controlling rights-of-access, e.g., a data service center in the DAB, in the case of indirect clearing, the service center sends an EMM clearing signal, specifically allocated to this security module, either via the telephone or a data communications system, to the service provider, and, there, feeds this EMM clearing signal for the service in question into a control unit of the service provider, and the security module is activated via the control unit by this EMM clearing signal assigned to it, or, in the case of direct clearing, the service center, with the aid of a data transmission service in a digital broadcasting service, such as the DAB single-frequency network, transmits the specifically assigned EMM clearing signal to the security module of the customer making the request and clears this customer. [The underlying advantage of the present invention is that, in]

In the case of a direct clearing, a service on a security module, such as a smart card, can be cleared by the particular transmission system, such as by using commercial DAB or DVB receivers themselves, or, in the case of an indirect clearing, with the aid of another service, besides the transmitting service. Following payment of the relevant data service fee, the service center assigns the entitlement by implementing a direct or indirect clearing, as mentioned above, via the smart-card specific EMM. A control unit set up at the service provider confirms activation of the security module, for instance of a smart card, for the service in question.

In another exemplary embodiment and/or exemplary method of the present invention, in the case of direct and indirect clearing, an electronically stored, service-specific credit balance (tokens) [can be advantageously] are allocated in monetary units to the security module.

In another exemplary embodiment and/or exemplary method of the present invention, in the case of indirect clearing of the security module of the querying customer, the data transmission service [can] is believed to be advantageously carried out, e.g., via a fixed-line modem, via a GSM[] (Global System for Mobile Communications) modem or via GSM-SMS services[] (where SMS is an acronym for "Service Management System").

In the case of direct clearing of the querying customer's security module, [it is also beneficial that] the approximate location of the customer can be found with the assistance of the cellular network, for example, the GSM network, [he or she] the customer is using. The specific EMM clearing signal for clearing the customer can be routed just within the DAM single-frequency network, where the customer is located at the time of the call and of the ordering of the EMM clearing signal.

[In this manner, the objectives mentioned above are achieved through implementation of] An exemplary embodiment and/or exemplary method of the present invention may implement a backward channel using GSM. In this regard, the sequence is described based on the DAB example:

- [
 1.] (i) From his or her automobile, via GSM, for example, the customer signals the data service center in the DAB requesting a clearing, for example, for a single data service or for a subscription, or in the case of non-receipt, [] a clearing, or an allocation of electronic, service-specific credit (tokens) on the smart card. [
 - [2.] (ii) In the data service center in the DAB, in collaboration, for example, with a GSM carrier[(], e.g., T-Mobil[]], the GSM cell[(], respectively, in this

manner, the DAB single-frequency network that covers a wider area[]], is determined in which the caller is located at the very moment. [

]

5 [3.] (iii) The relevant EMM is routed, with the clearing, to the DAB single-frequency network where the subscriber is located.[

]

10 [The advantages of the] An exemplary embodiment and/or method [in accordance with] of the present invention [can thus be seen, in particular, in] may further provide that there is no need to broadcast EMMs on a country-wide basis, but still only locally in the DAB service areas where the subscriber is also
15 located. [T] It is believed that this makes the data rate required for the EMMs substantially lower. In the case of a call, it is ensured that the caller can also receive the EMM, since, from an established GSM connection, one can infer the possibility of DAP reception. [Another important advantage lies in the fact that] Further, according to an exemplary
20 embodiment and/or exemplary method of the present invention, a backward channel [is] can be provided for new services.

In this context, the EMMs are not sent, for example, over a
25 GSM channel, since this would presuppose a data connection between the mobile telephone and the DAB receiver, which is, however, theoretically conceivable.

[Industrial Applicability

30]The exemplary embodiment and/or exemplary method in accordance with the present invention is believed to ha[s]ve industrial applicability, in particular for clearing customer-specific access entitlements in Conditional Access
35 Systems to enable chargeable media services to be received.

[] Abstract [

10 Of The [present invention is directed to a] Disclosure

5 A method for clearing customer-specific entitlements[] in
conditional access systems, to receive chargeable media
services, with the use of security modules, such as smart
cards, on which security algorithms and/or customer-specific
entitlements are stored in the form of software programs. In
10 response to a request from a service provider, such as a
T-Point or other institution authorized to sell security
modules, [
] in an indirect clearing, the service center responsible for
controlling entitlements sends an EMM clearing signal,
15 specifically allocated to this security module, either via the
telephone or a data communications system, to the service
provider, where this EMM clearing signal for the media service
in question is fed into a control unit of the service
provider, and the security module is activated via the control
20 unit by this EMM clearing signal assigned to it. [
] In a direct clearing, the service center, with the
assistance of a further data transmission service in a digital
broadcasting service, such as the DAB single-frequency
network, transmits the specifically assigned EMM clearing
25 signal to the security module of the customer making the
request and clears this customer.

[2345/153]

METHOD FOR CLEARING CUSTOMER-SPECIFIC ENTITLEMENTS ON SECURITY
MODULES IN CONDITIONAL ACCESS SYSTEMS FOR PAY SERVICES

Field of the Invention

The present invention is directed to a method for clearing customer-specific entitlements in conditional access systems, to receive chargeable services, such as pay TV, digital broadcasting data services in the DAB, DVB, Swift, video-on-demand, as well as any other digital services broadcast via radio broadcasting systems, with the use of security modules, such as smart cards, on which security algorithms and/or customer-specific entitlements are stored in the form of software programs and data, according to the definition of the species in Claim 1.

Background Information

Security modules in the form of smart cards are already in use today in many sectors where people, or machines as well, need to be granted authorized or conditional access [conditional access (CA systems)] to data, programs, or to other machines, when stipulated conditions or entitlements are satisfied (e.g., pay TV). Other typical areas of application for smart cards include electronic payment arrangements, GSM telephony, or digital broadcasting data services in the DAB, DVB, Swift, and also, in the future, video-on-demand.

In modern conditional access systems, access is controlled almost exclusively through the use of smart cards that utilize chip card technology. These smart cards contain stored security algorithms and customer-specific entitlements to receive fee-based data services. In conditional access systems, content providers encounter the problem of certainly wanting to reach more than one customer, but not all of them.

Only authorized customers should be able to receive a service. These are customers who meet stipulated conditions by purchasing entitlements, for example by paying a monthly subscriber fee. Radio broadcast systems are used to transmit entitlements of this kind. Therefore, there is a need to control access to certain information which is disseminated over broadcasting systems, but, in principle, can be received by everyone.

Conditional access systems, such as pay TV, protect such information from unauthorized access by scrambling, i.e., encrypting the program contents, by storing receive entitlement in the terminal's security module, and by adding receive conditions to the program. The terminals usually used to receive a pay TV program are the so-called set-top boxes or decoders. Other types of terminals are also possible, such as mobile receivers, PC cards, or PCMCIA modules. The terminal can also be integrated in the television set. In many cases, however, the lack of a way to guarantee receipt makes the clearing of smart cards problematic in broadcast systems, particularly when they are used in mobile devices for receiving services that do not feature point-to-point connections, as telephones do. A customer cannot utilize a desired service until the card is cleared, immediately following acquisition of the card. However, the sender of a clearing usually does not have any information on whether his clearing was actually received by the customer. A clearing is not effected when the unit being used is not able to receive a broadcast. This is the case, for example, in underground garages shielded by buildings, or when a radio communications network needed for sending out entitlements is not yet completely built up. In these cases, entitlements, constituted as so-called EMM messages (Entitlement Management Messages), cannot be received on an area-wide basis. In contrast, a controlled first clearing, including acknowledgment message, is very reliable and also renders possible an instantaneous collection of charges for the cleared service at the instant

of its acquisition.

Program contents are scrambled, in that the data are encoded by an encryption algorithm, with the control of a so-called control word CW. The algorithm mainly used in Europe for digital television based on the MPEG-2 standard is the DVB common scrambling algorithm. Other algorithms are also possible, however, such as DES or triple DES, inter alia (see Bruce Schneier, Angewandte Kryptographie, Wiley, 1996).

In so-called Entitlement Control Messages (ECM), a decoder or other receiver module is not only informed of new control words (CW), but also of the conditions under which a program may be received. Since both the CW, as well as the receive conditions, depend on the particular service, ECMs are allocated to each service. Once an ECM is received, it is directly routed to the security module. The control word CW must be transmitted confidentially. To protect the ECM, cryptographic methods are employed. Since the ECMs are sent to all customers, all authorized customers must possess the same key in order to decode the control word cryptogram. This is referred to as service key SK. The control word CW should be changed at relatively brief intervals, to make it impossible to recognize scrambling patterns.

Entitlement Management Messages (EMM) are used to set and to change receive entitlements stored in the decoder or in the security module. EMM messages must be sent to the individual address of the customer (respectively, of the decoder or of the security module). The customer's address and EMM messages must be protected from change; it must be ensured that only the program provider is able to generate EMM messages. Individual addresses always appear in the EMM messages as unencrypted messages; piracy protection can only be achieved by using supplementary information that is stored so as to be unreadable for the customer. This is the personal key (PK), which is linked to the customer address. EMM messages are sent

via the same broadcast system as the payload data. EMM messages are not permanently linked to the program content, but rather to the logical address of the customer's terminal, respectively to that of the security module, so that EMM can be addressed to individual customers or to groups of customers. Moreover, for the use of specific services, such as mobile received services or pay-per-view, a backward channel can be available, which is either implemented manually (call at a service center) or automatically (e.g., connection from the decoder to the transmission center via TCP/IP).

Entitlements can change when, for example, customers' chargeable accounts are not settled. The consequence of this can be the blocking of a receive authorization, for example. EMMs can also be used, however, for activating or reactivating services on smart cards. In these cases, the entitlements must be reset in the security module, such as the smart card. Today, as security modules, chip cards are mostly used which are not permanently connected to the terminal, but rather which can be removed from the terminal and replaced.

Reference is made to the related art publication in Bernd Seiler (publisher): taschenbuch der telekom praxis, 1996, Schiele & Schön Berlin 1996, Jörg Schwenk: "Conditional Access" or "Wie kann man den Zugriff auf Rundfunksendungen kontrollieren?".

Moreover, with the introduction of new transmission media, such as DAB and DVB-T, pay services are gaining in importance for mobile customers, as well. These are customers, who, for example, carry a terminal along with them in their automobile. Here, however, the following problems arise:

- the data capacity of the services is limited (e.g., DAB, Swift, inter alia);
- the receive situation is difficult (e.g., not yet fully developed broadcasting networks or automobiles located in

- underground garages); or
- a backward channel is normally not available.

Technical Objective

5

10

The object of the present invention is, therefore, to provide a method which will make it possible for an authorized customer's chip card to be made individually addressable to facilitate any change in pay services, the intention also being to make the pay services serviceable for mobile customers as well.

Summary of the Invention

15

20

25

30

35

The object is achieved in that, in response to a request from a service provider, i.e., an institution, such as a T-Point, authorized to issue or sell security modules, to a service center responsible for controlling rights-of-access, e.g., a data service center in the DAB, in the case of indirect clearing, the service center sends an EMM clearing signal, specifically allocated to this security module, either via the telephone or a data communications system, to the service provider, and, there, feeds this EMM clearing signal for the service in question into a control unit of the service provider, and the security module is activated via the control unit by this EMM clearing signal assigned to it, or, in the case of direct clearing, the service center, with the aid of a data transmission service in a digital broadcasting service, such as the DAB single-frequency network, transmits the specifically assigned EMM clearing signal to the security module of the customer making the request and clears this customer. The underlying advantage of the present invention is that, in the case of a direct clearing, a service on a security module, such as a smart card, can be cleared by the particular transmission system, such as by using commercial DAB or DVB receivers themselves, or, in the case of an indirect clearing, with the aid of another service, besides

the transmitting service. Following payment of the relevant data service fee, the service center assigns the entitlement by implementing a direct or indirect clearing, as mentioned above, via the smart-card specific EMM. A control unit set up at the service provider confirms activation of the security module, for instance of a smart card, for the service in question.

In the case of direct and indirect clearing, an electronically stored, service-specific credit balance (tokens) can be advantageously allocated in monetary units to the security module.

In the case of indirect clearing of the security module of the querying customer, the data transmission service can be advantageously carried out, e.g., via a fixed-line modem, via a GSM modem or via GSM-SMS services.

In the case of direct clearing of the querying customer's security module, it is also beneficial that the approximate location of the customer can be found with the assistance of the cellular network, for example the GSM network, he or she is using. The specific EMM clearing signal for clearing the customer can be routed just within the DAM single-frequency network, where the customer is located at the time of the call and of the ordering of the EMM clearing signal.

In this manner, the objectives mentioned above are achieved through implementation of a backward channel using GSM. In this regard, the sequence is described based on the DAB example:

1. From his or her automobile, via GSM, for example, the customer signals the data service center in the DAB requesting a clearing, for example, for a single data service or for a subscription, or in the case of non-receipt, a clearing, or an allocation of electronic, service-specific credit (tokens) on the smart card.

2. In the data service center in the DAB, in collaboration,
for example, with a GSM carrier (e.g., T-Mobil), the GSM
cell (respectively, in this manner, the DAB
single-frequency network that covers a wider area) is
determined in which the caller is located at the very
moment.
3. The relevant EMM is routed, with the clearing, to the DAB
single-frequency network where the subscriber is located.

The advantages of the method in accordance with the present
invention can thus be seen, in particular, in that there is no
need to broadcast EMMs on a country-wide basis, but still only
locally in the DAB service areas where the subscriber is also
located. This makes the data rate required for the EMMs
substantially lower. In the case of a call, it is ensured that
the caller can also receive the EMM, since, from an
established GSM connection, one can infer the possibility of
DAB reception. Another important advantage lies in the fact
that a backward channel is provided for new services.

In this context, the EMMs are not sent, for example, over a
GSM channel, since this would presuppose a data connection
between the mobile telephone and the DAB receiver, which is,
however, theoretically conceivable.

Industrial Applicability

The method in accordance with the present invention has
industrial applicability, in particular for clearing
customer-specific access entitlements in Conditional Access
Systems to enable chargeable media services to be received.

What is claimed is:

1. A method for clearing customer-specific entitlements in conditional access systems, to receive chargeable services, such as pay TV, digital data transmitted via radio broadcasting in DAB, DVB, Swift, video-on-demand, with the use of security modules, such as smart cards, on which security algorithms and/or customer-specific entitlements are stored in the form of software programs and data, wherein, in response to a request from a service provider, i.e., an institution authorized to sell security modules, to a service center responsible for controlling rights-of-access, in an indirect clearing, the service center sends an EMM clearing signal, specifically assigned to this security module, either via the telephone or a data communications system, to the service provider, and, there, feeds this EMM clearing signal for the media service in question into a control unit of the service provider, and the security module is activated via the control unit by this EMM clearing signal assigned to it, or, in a direct clearing, the service center, with the assistance of a data transmission service in a digital broadcasting service, transmits the specifically assigned EMM clearing signal to the security module of the customer making the request and clears this customer.

2. The method as recited in Claim 1, wherein in the case of direct and indirect clearing, an electronically stored, service-specific credit balance (tokens) can be advantageously allocated in monetary units to the security module.

3. The method as recited in Claim 1,
wherein in the case of indirect clearing of the security
module of the querying customer, the data transmission service
can optionally be carried out via a fixed-line modem, a GSM
modem, or via GSM-SMS services.

4. The method as recited in Claim 1 or 2,
wherein in the case of direct clearing of the security module
of the querying customer, the approximate location of the
customer is found with the assistance of a digital cellular
network, and the specific EMM clearing signal for clearing the
customer is only routed into the digital broadcasting network
in which the customer is situated at the time of the call and
of the ordering of the EMM clearing signal.

Abstract

The present invention is directed to a method for clearing customer-specific entitlements in conditional access systems, to receive chargeable media services, with the use of security modules, such as smart cards, on which security algorithms and/or customer-specific entitlements are stored in the form of software programs. In response to a request from a service provider, such as a T-Point or other institution authorized to sell security modules, in an indirect clearing, the service center responsible for controlling entitlements sends an EMM clearing signal, specifically allocated to this security module, either via the telephone or a data communications system, to the service provider, where this EMM clearing signal for the media service in question is fed into a control unit of the service provider, and the security module is activated via the control unit by this EMM clearing signal assigned to it. In a direct clearing, the service center, with the assistance of a further data transmission service in a digital broadcasting service, such as the DAB single-frequency network, transmits the specifically assigned EMM clearing signal to the security module of the customer making the request and clears this customer.



[2345/153]

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **METHOD FOR CLEARING CUSTOMER-SPECIFIC ENTITLEMENTS ON SECURITY MODULES IN CONDITIONAL ACCESS SYSTEMS FOR PAY SERVICES**, the specification of which was filed as International Application No. PCT/EP00/08263 on August 24, 2000 and filed as a U.S. application having Serial No. 09/830784 on May 1, 2001.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

Number	Country Filed	Day/Month/Year	Priority Claimed Under 35 USC 119
199 41 550.1	Fed. Rep. of Germany	01 September 1999	Yes

3-

And I hereby appoint Richard L. Mayer (Reg. No. 22,490), Gerard A. Messina (Reg. No. 35,952) and Linda M. Shudy (Reg. No. 47,084) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

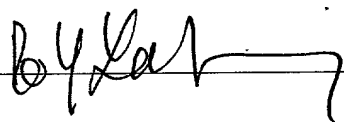
KENYON & KENYON
One Broadway
New York, New York 10004
CUSTOMER NO. 26646



Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

100
Inventor: Rolf LAKOMY

Inventor's Signature: 

Date: 11.06.2001

Residence: Hagenkamp 306
D-48308 Senden
Federal Republic of Germany DEX

Citizenship: German

Post Office Address: Same as above.

Inventor: **Joerg SCHWENK**

200

Inventor's Signature: _____

Joerg Schwenk

Date: 19/06/2001

Residence: Suedwestring 27
D-64807 Dieburg
Federal Republic of Germany *DEX*

Citizenship: German

Post Office Address: Same as above.